

DCMTK - Bug #1170

Issue when rendering an invalid monochrome DICOM image where the number of pixels stored does not match the expected number of pixel

2025-11-06 17:29 - Marco Eichelberg

Status:	Closed	Start date:	2025-11-06
Priority:	Normal	Due date:	
Assignee:	Jörg Riesmeier	% Done:	100%
Category:		Estimated time:	0:00 hour
Target version:		Compiler:	
Module:			
Operating System:			
Description			
There is an issue when rendering an invalid monochrome DICOM image where the number of pixels stored does not match the expected number of pixels. In this case, only a single pixel is processed, but the pixel matrix is much larger. Filling the rest of the pixel matrix with the smallest possible value for the image is not working because of an optimized memory usage (value would be out of range).			
Thanks to Ding zhengzheng < xiaozheng.ding399@gmail.com > for the report and the sample file (PoC).			
Closed by commit #410ffe201.			
This issue was registered as CVE-2025-25472 (https://www.cve.org/CVERecord?id=CVE-2025-25472).			